Discrete Applied Mathematics 297 (2021) 102–108

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Packing of permutations into Latin squares

Stephan Foldes [a], András Kaszanyitzky [b], László Major [c,*]

[a] University of Miskolc, 3515 Miskolc-Egyetemvaros, Hungary
[b] Eötvös Loránd University, Museum of Mathematics, 1117 Budapest, Pázmány Péter sétány 1/a, Hungary
[c] University of Turku, Faculty of Science and Engineering, 20500 Turku, Vesilinnantie 5, Finland

ARTICLE INFO

Article history:
Received 4 August 2020
Received in revised form 28 February 2021
Accepted 2 March 2021
Available online 31 March 2021

Keywords:
Latin square
Permutation group
Mutually orthogonal Latin squares
Centrosymmetric matrix

ABSTRACT

For every positive integer n greater than 4 there is a set of Latin squares of order n such that every permutation of the numbers $1, \ldots, n$ appears exactly once as a row, a column, a reverse row or a reverse column of one of the given Latin squares. If n is greater than 4 and not of the form p or $2p$ for some prime number p congruent to 3 modulo 4, then there always exists a Latin square of order n in which the rows, columns, reverse rows and reverse columns are all distinct permutations of $1, \ldots, n$, and which constitute a permutation group of order $4n$. If n is prime congruent to 1 modulo 4, then a set of $(n-1)/4$ mutually orthogonal Latin squares of order n can also be constructed by a classical method of linear algebra in such a way, that the rows, columns, reverse rows and reverse columns are all distinct and constitute a permutation group of order $n(n-1)$.

1. Introduction

A *permutation* is a bijective map f from a finite, n-element set (the domain of the permutation) to itself. When the domain is fixed, or it is an arbitrary n-element set, the group of all permutations on that domain is denoted by S_n (*symmetric group*). If the elements of the domain are enumerated in some well defined order as $z_1, \ldots, z_n$, then the sequence $f(z_1), \ldots, f(z_n)$ is called the *sequence representation* of the permutation f. This sequence representation then fully determines the permutation, and the term "permutation" may mean this sequence itself or the bijective map that it represents.

Without loss of generality we shall throughout this paper assume that matrix entries and the elements of the domain being permuted belong to some non-trivial ring with a zero and a unit element 1. This will allow in particular the multiplication of any square matrix of order n with the *reversal matrix* (also called the *exchange matrix*) of order n given by $J(i,j) = \delta_{i,n+1-j}$ (where $\delta_{i,j}$ is the Kronecker delta). For every n-by-n square matrix L, the columns of the conjugate JLJ are the *reverse columns* of L and the columns of the conjugate transpose JL^TJ are the *reverse rows* of L. The at most $4n$ sequences of length n occurring in L as rows, columns, reverse rows or reverse columns will be called *lines* of the matrix.

The four matrix operators mapping L to L, L^T, JLJ, and JL^TJ, respectively, form a group under composition. The matrix L is *symmetric* if $L = L^T$, *centrosymmetric* if $L = JLJ$ and *Hankel symmetric* if $L = JL^TJ$. None of these properties implies the others, but any two of them imply the third: such matrices have been studied e.g. in [1,2,5,8].

The opposite of this situation is when the $4n$ lines of the matrix L are all distinct, in this paper we call such a matrix *strongly asymmetric*. In this paper we are interested in matrices that are actually Latin squares. For the general theory of Latin squares see Keedwell and Dénes [7].

* Corresponding author.
E-mail addresses: foldes.istvan@uni-miskolc.hu (S. Foldes), kaszi75@gmail.com (A. Kaszanyitzky), laszlo.major@utu.fi (L. Major).

https://doi.org/10.1016/j.dam.2021.03.001
0166-218X/

Given a finite, n-element set R, a set S of m Latin squares of order n with entries in R (meaning that each line of each member of S represents a permutation of R) is called a *packing* if

(i) all members of S are strongly asymmetric,
(ii) no line of any member of S appears as a line in any other member of S.

Equivalently, S is a packing if the number of distinct sequences appearing as lines in the members of S is $4nm$. In that case the $4nm$ permutations represented by these $4nm$ sequences are said to be *packed into* the set S of Latin squares.

Proposition 1. *If some subgroup G of the symmetric group S_n of all permutations is packed into a set S of strongly asymmetric Latin squares, then every subgroup H of S_n containing G is also packed into some set of strongly asymmetric Latin squares.*

Proof. Let Q be a set of $|H|/|G|$ distinct representatives of the (left) cosets of G in H. Apply each representative to each matrix M in S elementwise, i.e. for each q in Q and each M form the matrix qM given by $(qM)(i, j) = q(M(i, j))$. □

2. Packing into Latin squares of odd order

Fact 1. *Let C and R be subgroups of a group G. For any element $g \in G$ the following conditions are equivalent:*

(i) the map from the Cartesian product set $C \times R$ to the double coset CgR that sends (c, r) to cgr is bijective,
(ii) the conjugate subgroup gRg^{-1} intersects C trivially.

Fact 2. *Let C and R be subgroups of a finite group G. The following conditions are equivalent:*

(i) all the double cosets have cardinality equal to $Card(C)\times Card(R)$,
(ii) every conjugate of C meets every conjugate of R trivially.

Fact 3. *Let C and R be two subgroups of a finite group G whose orders are relatively prime. Then all the double cosets have cardinality equal to $Card(C)\times Card(R)$.*

The following theorem will be proved by an appropriate application of the "addition square" construction appearing in Gilbert [6].

Theorem 1. *If n is a positive odd number at least 5, then the symmetric group S_n can be packed into some set of strongly asymmetric Latin squares.*

Proof. Fact 3 applies in particular if G is the symmetric group of all permutations of the n-element set $\{1, \ldots, n\}$, for odd $n \geq 5$, C is the subgroup generated by the circular shift permutation whose sequence representation is $(2, \ldots, n, 1)$, and R is the two-element subgroup containing the reversal permutation whose sequence representation is $(n, \ldots, 1)$.

All double cosets CgR have cardinality $2n$. The number $(n-1)!/2$ of double cosets is even. Arrange the double cosets in matched pairs. From each matched pair (A, B) of double cosets choose representatives p, q from A, B, respectively. Construct the matrix M given by $M(i, j) = p(i) + q(j)$, where addition is modulo n.

The columns and reverse columns of M are precisely the members of the double coset A, and the rows and reverse rows of M are the members of the double coset B. In the set of $(n-1)!/4$ matrices so constructed every permutation occurs exactly once as a row, column, reverse row or reverse column. □

Remark 1. The above construction does not work for even n, because the circular shift applied $n/2$ times is then a conjugate of the reversal (has similar cyclic structure).

3. Packing into Latin squares of even order

Definition 1. An m-by-m matrix (possibly Latin square) is called a *double occurrence matrix* if every sequence appearing as a line (row, column, reverse row, or reverse column) appears exactly twice. A set of double occurrence matrices is called a *double occurrence matrix set* if no sequence appears as a line in more than one of the matrices. The set of permutations whose sequence representations appear as lines in a double occurrence matrix or matrix set is called the *set covered* by the matrix or matrix set.

Proposition 2. *For every $m > 2$ there is a double occurrence matrix set covering all permutations of* $1, \ldots, m$.

Proof. First we observe that for every $m > 2$, there is an m-by-m double occurrence matrix such that the lines appearing in the matrix constitute the sequence representations of a permutation group on the numbers $1, \ldots, m$. Indeed, such a matrix can be defined by letting the element of the matrix in row i and column j be the number $i + j$, with addition defined modulo m.

$$
\mathrm{L} = \begin{array}{|c|c|c|}\hline 1 & 3 & 2 \\ \hline 2 & 1 & 3 \\ \hline 3 & 2 & 1 \\ \hline \end{array}
\qquad
\mathrm{A} = \begin{array}{|c|c|c|}\hline 1 & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline 0 & 1 & 0 \\ \hline \end{array}
\qquad
\longrightarrow L * A = \begin{array}{|c|c||c|c||c|c|}\hline 2 & 1 & 5 & 6 & 4 & 3 \\ \hline 1 & 2 & 6 & 5 & 3 & 4 \\ \hline\hline 3 & 4 & 1 & 2 & 6 & 5 \\ \hline 4 & 3 & 2 & 1 & 5 & 6 \\ \hline\hline 5 & 6 & 4 & 3 & 1 & 2 \\ \hline 6 & 5 & 3 & 4 & 2 & 1 \\ \hline \end{array}
$$

Fig. 1. An example of constructing a composite matrix.

Secondly, let M be any m-by-m double occurrence matrix whose lines constitute a permutation group G. Let R be any complete system of representatives of the left cosets of G in the symmetric group of all permutations of $1, \ldots, m$. Applying the various permutations $r \in R$ (viewed as functions) entrywise to M we obtain the matrix set required. □

Remark 2. The matrix set whose existence is stated in Proposition 2 necessarily consists of $m!/2m = (m-1)!/2$ matrices.

For $k = 1, \ldots, m$ let the 2-by-2 matrices B_{k_0} and B_{k_1} be defined as

$$B_{k_0} = \begin{bmatrix} 2k-1 & 2k \\ 2k & 2k-1 \end{bmatrix} \quad B_{k_1} = \begin{bmatrix} 2k & 2k-1 \\ 2k-1 & 2k \end{bmatrix}$$

For an m-by-m Latin square L and each m-by-m Boolean matrix A ($0-1$ matrix), let the $2m$-by-$2m$ *composite matrix* $L * A$ be defined by replacing each entry of L in row i and column j whose value is k by the 2-by-2 block $B_{k_{A(i,j)}}$ (for an example see Fig. 1).

Remark 3. Both L and A are encoded into the composite $L * A$ without loss of information: $A(i, j)$ is 0 or 1 according to whether $(L * A)(2i-1, 2j-1)$ is smaller or larger than $(L * A)(2i-1, 2j)$, and $L(i, j)$ is half the larger of these two entries of $L * A$.

Proposition 3. *For every even number $2m > 4$, there is a set S of Latin squares of order $2m$, such that every sequence representing a permutation preserving the partition of the numbers $1, 2, \ldots, 2m-1, 2m$ into pairs of consecutive numbers occurs exactly once as a line of some member of S.*

Remark 4. The set of permutations packed into the set S of Latin squares according to this proposition constitutes a subgroup of order $m!\, 2^m$ of the symmetric group S_{2m}.

Proof. Partition into pairs $\{v, w\}$ in any manner the set of $0-1$ vectors of length m whose first component is 0 (actually partitioning into pairs of any complement-free set of 2^{m-1} vectors will do). Order each pair $\{v, w\}$ arbitrarily into an ordered pair (v, w). For each such ordered pair define the m-by-m Boolean matrix A_{vw} by $A_{vw}(i, j) = v(i) + w(j)$, with addition modulo 2.

We obtain thus a set of 2^{m-2} Boolean matrices with the property that if a vector v appears as the ith row in one of the matrices, then the ith column of that matrix is neither v nor its Boolean complement.

Let E be a double occurrence matrix set covering all permutations of $1, \ldots, m$, which exists according to Proposition 2 and consists of $(m-1)!/2$ matrices.

Let S consist of all the composite matrices $(L * A)_{vw}$, where L can be any member of E and A_{vw} is any of the 2^{m-2} Boolean matrices defined above. In view of Remark 3, the set S consists of $(m-1)!\, 2^{m-3}$ matrices. The key to verifying that no vector can appear twice as a line anywhere in S, is to note that because of the double occurrence property of E the only possible coincidences to worry about concern rows and columns of the same member matrix of S, but such coincidences are excluded due to the complement-free property of the set of Boolean vectors used to define the matrices A_{vw}.

The proof is concluded by observing that the number of (distinct) lines appearing in members of S is $(m-1)!\, 2^{m-3} \cdot 8m = m!\, 2^m$, which is the number of the partition-preserving permutations specified in the statement of the proposition. □

Theorem 2. *If n is a positive even number at least 6, then the symmetric group S_n can be packed into some set of strongly asymmetric Latin squares.*

Proof. Proposition 3 packs a subgroup of the symmetric group. Combining with Proposition 1 yields the result. □

4. Packing a permutation group into a single Latin square

In this section we give a construction showing that if n is either a composite odd integer or a prime congruent to 1 mod 4, then the symmetric group S_n has a subgroup — necessarily of order $4n$ — that can be packed into a single strongly asymmetric Latin square. The construction will use basic properties of finite rings, where by a ring we always mean a commutative ring with unit element 1.

In any ring the equation $2x = 1$ has at most one solution. It follows that the *reflection in the identity* mapping every element x to $1 - x$ has at most one fixed point. This reflection is an involution, as a permutation it is a product of disjoint transpositions. Note that in a finite, n-element ring the reflection has a fixed point if and only if n is odd.

An enumeration $z_1, \dots, z_n$ of the elements of a finite n-element ring is called *reflectable* if $z_i' = z_{n-i+1}$ for all i.

Proposition 4. *Every finite ring has a reflectable enumeration of its elements.*

Proof. If the reflection has no fixed point, n is even and the elements of R can be partitioned into $n/2$ pairwise disjoint pairs so that the reflection exchanges the elements of each pair. Choose in any way one element from each pair and enumerate them in any order as $z_1, \dots, z_{n/2}$. Then let $z_{n-i+1} = z_i'$ for $i = 1, \dots, n/2$.

If the reflection has a fixed point y, then the other elements of R can be partitioned into $(n-1)/2$ pairwise disjoint pairs so that the reflection exchanges the elements of each pair. Again, choose in any way one element from each pair and enumerate them in any order as $z_1, \dots, z_{(n-1)/2}$. Let $z_{(n+1)/2} = y$ and let $z_{n-i+1} = z_i'$ for $i = 1, \dots, (n-1)/2$. □

Definition 2. We shall say that in a finite ring R a 4-element subgroup G of the multiplicative group of units is a *quartet* if it consists of two distinct elements and their negatives. (Necessarily 1 and -1 belong then to the quartet G, and R does not have characteristic 2.)

Proposition 5. *Let n be an integer at least 5. The following conditions are equivalent:*

(i) there exists an n-element commutative ring R with unit that has a quartet,
(ii) n is not a prime congruent to 3 mod 4, and it is not 2 times such a prime.

Proof. If (ii) does not hold but (i) does, then the additive group of R must be cyclic, therefore R is isomorphic to $\mathbb{Z}_n$. Euler's phi function takes value $n - 1$ on n, where n is a prime, or the value $(n/2) - 1$ if n is 2 times a prime, thus the order of the group of units of $\mathbb{Z}_n$ is not divisible by 4 and therefore it cannot have any 4-element subgroup, contradicting (i).

If (ii) holds, we need to examine the following cases.

Case 1: if n is composite odd, let $n = mq$ be a proper factorization. Obviously both m and q are greater then 2. The direct product ring $\mathbb{Z}_m \times \mathbb{Z}_q$ has a quartet, namely $(1, 1), (-1, -1), (1, -1), (-1, 1)$.

Case 2: if n is prime congruent to 1 mod 4 then in $\mathbb{Z}_n = GF(n)$ the element -1 has a square root r and $\{1, -1, r, -r\}$ is a quartet.

Case 3: if n is divisible by 4, then in $\mathbb{Z}_n$ the residues $1, -1, (n-2)/2$ and $(n+2)/2$ form a quartet.

Case 4: if n is of the form $2m$ where m is odd, then by applying Cases 1 and 2 we see that some m-element ring A has a quartet Q. Then in the direct product ring $\mathbb{Z}_2 \times A$ the set of elements of the form $(1, q)$, where q is in Q, is a quartet. □

Theorem 3. *If the integer $n > 4$ is not of the form p or $2p$ with prime p congruent to 3 modulo 4, then there exists a strongly asymmetric Latin square of order n the $4n$ distinct lines of which form a permutation group (subgroup of S_n).*

Proof. By Proposition 5 there exists an n-element commutative ring R with unit that has a quartet G. Let c, d be distinct elements of G such that c is not the negative of d, and let $z_1, \dots, z_n$ be a reflectable enumeration of the elements of R (with respect to an element u). Let the n-by-n matrix M be given by $M(i, j) = cz_i + dz_j$. We show that the $4n$ lines of the matrix M are all distinct.

A column of M is a sequence of the form

$$cz_1 + b, \dots, cz_n + b \tag{1}$$

for some element b of R. The corresponding reverse column is the sequence

$$cz_1' + b, \dots, cz_n' + b$$

which is $(-c)z_1 + (b + cu), \dots, (-c)z_n + (b + cu)$, i.e. it is in the form

$$(-c)z_1 + a, \dots, (-c)z_n + a \tag{2}$$

for some element a of R.

As for distinct columns the corresponding elements b in (1) are distinct, the columns of the matrix M are all distinct, and by a similar argument the rows of M are distinct from each other too.

If a column (1) were to coincide with a reverse column (2), then for all $i = 1, \ldots, n$ we would have $cz_i + b = (-c)z_i + a$. In particular, taking $z_i = 0$, we would have to have $a = b$, and then $z_i = -z_i$ for all i by the invertibility of c, implying in particular $1 = -1$, which is impossible. Thus no column is identical with a reverse column.

Suppose that a column (1) were to coincide with a row. The row would be of the form

$$e + dz_1, \ldots, e + dz_n \tag{3}$$

for some element e of R. For $i = 1, \ldots, n$ we would have $cz_i + b = e + dz_i$. Setting $z_i = 0$ would imply $e = b$. Then setting $z_i = 1$ would imply $c = d$, which is impossible. Thus no column is identical with a row.

If a column (1) were to coincide with the reverse of a row of the form (3), then the reverse column (2) would coincide with (3). Then for all we would have $(-c)z_i + a = e + dz_i$, implying $a = e$ and then $-c = d$, which is impossible by the choice of c and d. Thus no column is identical with a reverse row.

Summarizing what we have seen so far: no column is identical with any other line. Similarly we can conclude that no row is identical with any other line. □

When n is a prime congruent to 3 modulo 4, then the following proposition shows that no permutation group can be packed into a single Latin square of order n.

Proposition 6. *There is no order $4n$ subgroup in S_n for prime n congruent to 3 modulo 4.*

Proof. The statement is obvious for $n = 3$, so we may assume that the prime number n is at least 7. Suppose S_n has a subgroup H of order $4n$, we shall derive a contradiction.

As n is prime, by Cauchy's Theorem (a precursor of Sylow's) H has a subgroup C of order n. The subgroup C must be normal in H because any two distinct conjugates of C in H would generate together a subgroup of order at least $n^2 > 4n$, which is impossible, again because n is at least 7. By Sylow's Theorem, H also has a subgroup D of order 4. This 4-element group D acts on C by conjugation. (As also apparent from the applicability of the Schur–Zassenhaus Theorem to H based on the prime power decomposition of its order $4n$.)

We claim that the conjugations by the elements of D are all distinct, thus constituting a 4-element subgroup of the automorphism group $\mathrm{Aut}(C)$. For this it suffices to see, because D and C only have the identity element in common, that the centralizer of C in S_n is C itself. This follows from the fact that there are exactly $(n-1)!$ permutations in S_n that are n-cycles and they are all conjugate in S_n. The intended contradiction is now obtained observing that C being a cyclic group of prime order n congruent to 3 mod 4, its automorphism group $\mathrm{Aut}(C)$ has order $n-1$ congruent to 2 mod 4, thus $n-1$ is not divisible by 4, and therefore $\mathrm{Aut}(C)$ cannot have a 4-element subgroup. □

Finally, if n is of the form $2p$ with p prime congruent to 3 modulo 4, then subgroups of order $4n$ do exist in S_n according to the following proposition, but we do not know if any such subgroup can be packed into a Latin square.

Proposition 7. *For even integers $n = 2m \geq 6$ the symmetric group S_n always has a subgroup of order $4n$.*

Proof. For any integer $m \geq 4$ let us consider the subgroup consisting of permutations f defined on the set $\{1, \ldots, m, m+1, \ldots, 2m\}$ for which

(i) each of the sets $\{1, \ldots, m\}$, $\{m+1, m+2\}$ and $\{m+3, m+4\}$ is invariant under the permutation f,
(ii) every $i \in \{m+5, \ldots, 2m\}$ is a fixed point of f,
(iii) there exist an i and a $k \in \{-1, 1\}$ such that for every $j \in \{1, \ldots, m\}$, $f(j)$ is congruent to $i + kj$ modulo m.

The number of permutations in this subgroup — isomorphic to the direct product $D_m \times \mathbb{Z}_2^2$ of a dihedral group and the Klein group — is indeed $2^3 m = 4n$.

For the case $m = 3$ let us consider the subgroup of order $4n = 24$ consisting of permutations f defined on the set $\{1, \ldots, 6\}$ for which 5 and 6 are fixed points under f. □

5. Mutually orthogonal Latin squares

A pair of Latin squares L and L' of order n are *orthogonal* if for all $i, j \in \{1, \ldots, n\}$, the ordered pairs $(L(i,j), L'(i,j))$ are distinct. A set of Latin squares is called *mutually orthogonal* (MOLS) if each Latin square in the set is orthogonal to every other Latin square of the set.

Theorem 4. *For every prime number p congruent to 1 modulo 4, there is a permutation group G of order $(p-1)p$ and a set of $(p-1)/4$ mutually orthogonal Latin squares of order p such that every permutation in G occurs exactly once as a line of one of these Latin squares.*

Proof (*Method based on Bose [3]*). Let p be a prime number congruent to 1 mod 4, with the arithmetic of $GF(p)$ on the set $\{1, \ldots, p\}$. Using the subset $V = \{1, \ldots, (p-1)/2\}$ let us form $(p-1)/4$ ordered couples (r, s) so that every member of

V occurs exactly once as a (first or second) component of such a couple (r, s). It is easy to see that the couples can be formed in a way that for any two distinct couples (r, s) and (r', s') the determinant of the matrix

$$\begin{bmatrix} r & s \\ r' & s' \end{bmatrix}$$

is non-zero (for example take the couples $(r, r+(p-1)/4)$ for $r = 1, \ldots, (p-1)/4$). For each of these couples (r, s) define the p-by-p matrix M_{rs} by

$$M_{rs}(i, j) = ri + sj$$

The $(p-1)/4$ matrices so defined are mutually orthogonal. As the set V does not contain the negative of any of its members, every permutation of the elements of $GF(p)$ given by the linear permutation polynomial $f(x) = rx + c$, with $r \in V$ and $c \in GF(p)$, will occur exactly once as a row or column of one of the $(p-1)/4$ matrices given, and every permutation of the elements of $GF(p)$ given by $f(x) = rx + c$, with $r \in GF(p) - \{0\}$ and $c \in GF(p)$ will occur exactly once as a line of one of these matrices. Moreover, the $(p-1)p$ permutations having this linear (affine) form constitute a group. □

6. Minimum number of lines and symmetries of Latin squares

The question that is opposite to the one asking for as many distinct lines as possible in Latin squares is that of how many of the $4n$ lines of a Latin square of order n must be distinct. More precisely, let $min(n)$ be the first positive integer m such that every Latin square of order n has at least m distinct lines, and let $min(L)$ denote the number of distinct lines in a given Latin square L. By the very definition of Latin squares, $min(n)$ is obviously at least n. In this section we shall see that the value of $min(n)$ depends on the parity of n, and for a given Latin square L of order n, it depends on the symmetry properties of L whether $min(L) \geq min(n)$.

Theorem 5. *If $n > 1$ is odd, then every Latin square of order n has at least $2n$ distinct lines, and a Latin square of order n having $2n$ distinct lines exists. For even n, every Latin square of order n has at least n distinct lines, and a Latin square of order n having n distinct lines exists.*

Proof. If a Latin square of odd order $n > 1$ had less than $2n$ distinct lines, then some line would have to appear at least three times in L. It would then have to appear either both as a row and a reverse row, or both as a column and a reverse column. In the first case the middle elements of two rows would have to be the same, which is impossible in a Latin square, and the second case is ruled out similarly. On the other hand, given any $n > 1$ odd number, the matrix $M(i, j) = i + j - 1$ (with addition $\mod n$) is a Latin square with exactly $2n$ lines (see Proposition 2).

For the even case, we only need to show that for any even $n = 2m$ a Latin square of order n having only n distinct lines exists. Indeed, let A be a symmetric Latin square of order m. Let another m-by-m matrix B be defined by $B(i, j) = A(i, j)+m$. Then, with J denoting the $0-1$ matrix with 1's only on the Hankel diagonal (reversal matrix), the following matrix is a Latin square of order n having only n distinct lines:

$$\left[\begin{array}{c|c} A & BJ \\ \hline JB & JAJ \end{array}\right]$$

Note that this $n \times n$ matrix is symmetric and also centrosymmetric. The construction is similar to a construction for centrosymmetric Latin squares given in [4]. □

Theorem 6. *A Latin square L of odd order $n > 1$ has exactly $2n$ distinct lines if and only if L is symmetric or Hankel symmetric. A Latin square L of even order $n > 0$ has exactly n distinct lines if and only if L is both symmetric and Hankel symmetric.*

Proof. *For odd* $n = 2m - 1$: if L is symmetric, then each of the n rows also appears as a column. Therefore this same line cannot additionally also appear as a reverse row or a reverse column, because this would result in a coincidence of middle elements, which is impossible in a Latin square. It follows that reverse rows, also appearing by symmetry as reverse columns, make up an other set of n disjoint lines. Similarly, if L is Hankel symmetric, then each of the n rows appears as a reverse column and each of the n reverse rows appears as a column resulting in a total of $2n$ distinct lines.

To verify the converse, suppose that L has exactly $2n$ distinct lines. No column can appear as a reverse column. Thus the set of columns and reverse columns must contain $2n$ distinct lines. Each row must therefore appear in this set, i.e. each row must also appear either as a column or as a reverse column. Assume that the middle row appears as a column (necessarily as the middle column), but the ith row, for some $i \neq \frac{n+1}{2}$, appears as a reverse column, necessarily as the $(n-i+1)$th reverse column. In this case, the ith element of the middle column is the same as the $(n-i+1)$th element of the middle row, which is impossible. Consequently, for every $i = 1, \ldots, n$, the ith row appears as a column, and necessarily as the ith column, i.e. L is symmetric. If the middle row appears as a reverse column, then similarly we obtain that L is Hankel symmetric.

For even n: if L is both symmetric and Hankel symmetric, then it is also centrosymmetric, and every row must appear also as a column, as a reverse row and as a reverse column as well. There can be thus no more lines appearing in L than the n rows.

To see the converse, suppose that L has only n distinct lines. Each line must therefore appear 4 times: it must appear as a row, as a column, as a reverse row and as a reverse column as well. But the ith row can only appear as the ith column, and thus L must be symmetric. For a similar reason, the jth reverse row must appear as the reverse column that is the $(n - j + 1)$th from the left, and thus L is also Hankel symmetric. □

Acknowledgements

We thank the referees for their comments, in particular for suggesting simplified proofs for Proposition 6 and Theorem 6.

References

[1] I.T. Abu-Jeib, Centrosymmetric matrices: Properties and an alternative approach, Can. Appl. Math. Q. 10 (4) (2002) 429–445.
[2] A.L. Andrew, Centrosymmetric matrices, SIAM Rev. (1998) 697–699.
[3] R.C. Bose, On the application of the properties of galois fields to the problem of construction of hyper-Greco-Latin squares, Sankhya 3 (4) (1938) 323–338.
[4] R.A. Brualdi, L. Cao, Symmetric, Hankel-symmetric, and centrosymmetric doubly stochastic matrices, Acta Math. Vietnam. 43 (4) (2018) 675–700.
[5] A.B. Cruse, Some combinatorial properties of centrosymmetric matrices, Linear Algebra Appl. 16 (1) (1977) 65–77.
[6] E.N. Gilbert, Latin squares which contain no repeated digrams, SIAM Rev. 7 (2) (1965) 189–198.
[7] A.D. Keedwell, J. Dénes, Latin Squares and Their Applications, Elsevier, 2015.
[8] Z.-Y. Liu, Some properties of centrosymmetric matrices, Appl. Math. Comput. 141 (2–3) (2003) 297–306.